CWNA-109^Q&As^

Certified Wireless Network Administrator

Pass CWNP CWNA-109 Exam with 100% Guarantee

QUESTION 1

What is an advantage of using WPA3-Personal instead of WPA2-Personal as a security solution for 802.11 networks?

A. WPA3-Personal, also called WPA3-SAE, uses an authentication exchange and WPA2- Personal does not

B. WPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network

C. WPA3-Personal, also called WPA3-SAE, uses AES for encryption and WPA2-Personal does not

D. WPA3-Personal, also called WPA3-SAE, uses a better encryption algorithm than WPA2- Personal

Correct Answer: B

An advantage of using WPA3-Personal instead of WPA2-Personal as a security solution for 802.11 networks is that WPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network. WPA3Personal uses Simultaneous Authentication of Equals (SAE) as the key exchange protocol, which provides stronger protection against offline dictionary attacks and password guessing than WPA2-Personal. SAE uses a Diffie-Hellman key exchange with elliptic curve cryptography (ECC) to establish a pairwise master key (PMK) between the AP and the client without revealing it to any eavesdropper. SAE also provides forward secrecy, which means that if one PMK is compromised, it does not affect the security of other PMKs. WPA2-Personal uses Pre- Shared Key (PSK) as the key exchangeprotocol, which is vulnerable to offline brute-force attacks if the passphrase is weak or leaked. Both WPA3Personal and WPA2-Personal use AES for encryption, so there is no difference in that aspect. WPA3-Personal does not use a different encryption algorithm than WPA2-Personal, but rather a different key exchange protocol. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 297.

QUESTION 2

You are troubleshooting a client problem with a 2.4 GHz WLAN connection. The client is experiencing surprisingly low data rates during the work day. You analyze the workspace outside of business hours and detect a strong signal with a typical noise floor at the client location. During working hours, the user works with a laptop in the area and uses an external USB hard drive for continuous data access. The user also states that the laptop works as expected on her home network. The user working approximately 8 feet away from this client experiences no problems.

Based on this information, what is the likely cause of the problem?

A. The AP is overloaded during the work day

B. The drivers in the laptop are corrupt

C. The laptop has a failing wireless adapter

D. The external hard drive is USB 3.0 and is causing a significant increase in the noise floor when in use

Correct Answer: D

The likely cause of the problem is that the external hard drive is USB 3.0 and is causing a significant increase in the noise floor when in use. USB 3.0 devices are known to generate radio frequency interference (RFI) in the 2.4 GHz band due to their high data transfer rates and harmonics. This RFI can increase the noise floor and degrade the signal- to-noise ratio (SNR) of WLAN devices operating in the same band. This can result in lower data rates, reduced throughput, increased retransmissions, and poor performance. The problem may not occur outside of business hours or on the user\\'s home network because of different usage patterns or environmental factors. References: [CWNP Certified

Wireless Network Administrator Official StudyGuide: ExamCWNA-109], page 527; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 497.

QUESTION 3

The BSA of an AP covers the area used by the sales and marketing department. Thirty-five stations operate in this space. The users indicate that they need more throughput and all stations are 5 GHz capable 802.11ac clients. The current AP configuration uses 20 MHz channels in both 2.4 GHz and 5 GHz. What is the least expensive solution available for increasing throughput for these users without implementing configuration options that are not recommended?

A. Use a 160 MHz channel on the 5 GHz radio

B. Use a 40 MHz channel on the 5 GHz radio

C. Install a second AP in the coverage area

D. Use a 40 MHz channel on the 2.4 GHz radio

Correct Answer: B

The least expensive solution available for increasing throughput for these users without implementing configuration options that are not recommended is to use a 40 MHz channel on the 5 GHz radio. This solution can double the channel bandwidth and increase the data rates for the 5 GHz capable 802.11ac clients. Using a 40 MHz channel on the 5 GHz radio is also less likely to cause co-channel interference or overlap with other channels than using a 40 MHz channel on the 2.4 GHz radio, which has only three non-overlapping channels. Using a 160 MHz channel on the 5 GHzradio may provide even higher throughput, but it may also consume too much of the available spectrum and cause more interference with other devices or networks. Installing a second AP in the coverage area may also improve the throughput, but it may require additional costs and configuration. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 216; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 206.

QUESTION 4

A natural disaster has occurred in a remote area that is approximately 57 miles from the response team headquarters. The response team must implement a local wireless network using 802.11 WLAN access points. What is the best method, of those listed, for implementation of a network back-haul for communications across the Internet in this scenario?

A. 802.11 bridging to the response team headquarters

B. Cellular/LTE/5G

C. Turn up the output power of the WLAN at the response team headquarters

D. Temporary wired DSL

Correct Answer: B

Cellular/LTE/5G is the best method for implementing a network backhaul for communications across the Internet in a remote area that is affected by a natural disaster. This is because cellular/LTE/5G networks are wireless and do not depend on physical infrastructure that may be damaged or unavailable in such scenarios. Cellular/LTE/5G networks also offer high-speed data transmission and wide coverage area, which are essential for emergency response operations. 802.11 bridging to the response team headquarters is not feasible because it requires line-of-sight and has limited range. Turning up the output power of the WLAN at the response team headquarters is not effective because it may cause interference and does not guarantee reliable connectivity. Temporary wired DSL is not practical because it requires installing cables and equipment that may not be available or accessible in a remote area. References: CWNA-109 Study Guide, Chapter 7: Wireless LAN Topologies, page 2031

QUESTION 5

You recently purchased four laptops containing dual-band 802.11ac adapters. The laptops can connect to your 2.4 GHz network, but they cannot connect to the 5 GHz network. The laptops do not show the 5 GHz SSIds, which are different than the 2.4 GHz SSIDs. Existing devices can connect to the 5 GHz SSIDs with no difficulty. What is the likely problem?

A. Interference from non-Wi-Fi sources

B. Faulty drivers

C. DoS attack

D. Interference from other WLANs

Correct Answer: B

The likely problem that causes this scenario is faulty drivers. Drivers are software components that enable the communication between the operating system and the hardware devices, such as the wireless adapters. Faulty drivers can cause various issues with the wireless connectivity, such as not detecting or connecting to certain networks, dropping connections, or reducing performance. Faulty drivers can be caused by corrupted files, outdated versions, incompatible settings, or hardware defects. To fix faulty drivers, you can try to update, reinstall, or roll back the drivers, or contact the manufacturer for support. Interference from non-Wi-Fi sources, DoS attack, or interference from other WLANs are not likely to cause this scenario, as they would affect all devices in the same area, not just the new laptops. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 562; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 532.

QUESTION 6

What factor does not influence the distance at which an RF signal can be effectively received?

A. Receiving station\\'s radio sensitivity

B. Receiving station\\'s output power

C. Transmitting station\\'s output power

D. Free Space Path Loss

Correct Answer: B

In wireless communication, several factors influence the effective reception of RF signals, including the receiving station\\'s radio sensitivity, the transmitting station\\'s output power, and free space path loss. However, the receiving station\\'s

output power does not influence the distance at which an RF signal can be effectively received. The key factors that impact signal reception distance are:

Receiving Station\\'s Radio Sensitivity: This refers to the lowest signal strength at which the receiver can process a signal with an acceptableerror rate. Higher sensitivity allows for better reception at greater distances. Transmitting Station\\'s

Output Power: This is the power with which a transmitter sends out a signal. Higher output power can extend the range of transmission, making it easier for distant receivers to detect the signal. Free Space Path Loss (FSPL): FSPL

represents the attenuation of radio energy as it travels through free space. It increases with distance and frequency, reducing the signal strength as the distance from the transmitter increases. The output power of the receiving station is

related to how strong a signal it sends out, not how well it can receive or process incoming signals. Therefore, it does not affect the reception distance of incoming RF signals.

References:

CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0- 105, by David D. Coleman and David A. Westcott.

RF fundamentals and RF design considerations in wireless communication systems.

QUESTION 7

You are configuring an access point to use channel 128. What important fact should be considered about this channel?

A. It is a 2.4 GHz frequency band 40 MHz channel, so it should not be used

B. It is a 22 MHz channel so it will overlap with the channels above and below it

C. It is a channel that may require DFS when used

D. It is a channel that is unsupported by all access points in all regulatory domains

Correct Answer: C

It is a channel that may require DFS when used is an important fact that should be considered about channel 128. Channel 128 is a 5 GHz frequency band 20 MHz channel that has a center frequency of 5.64 GHz. Channel 128 is one of the channels that are subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. DFS is a feature that is defined in the IEEE 802.11h amendment and is mandated by some regulatory bodies, such as the FCC and the ETSI, to protect the licensed users of the 5 GHz band from interference by unlicensed Wi-Fi devices. DFS works by using a mechanism called channel availability check (CAC), which requires Wi-Fi devices to scan a channel for a certain period of time before using it. If a radar signal is detected during the CAC or while using the channel, the Wi-Fi devices must switch to another channel that is free from radar interference. When configuring an access point to use channel 128, it is important to consider the implications of DFS rules, such as: The access point must support DFS and comply with the local regulations and standards that apply to DFS channels. The access point may experience delays or interruptions in its operation due to CAC or channel switching. The access point may have limited channel selection or availability due to radar interference or other Wi-Fi devices using DFS channels. The access point may have compatibility or interoperability issues with some client devices that do not support DFS or use different DFS parameters. The access point may have performance or quality issues due to co-channel or adjacent-channel interference from other Wi-Fi devices using non-DFS channels. Therefore, it is advisable to use channel 128 only when necessary and after performing a thorough site survey and spectrum analysis to determine the best channel for the access point.
References: 1, Chapter 3, page 117; 2, Section 3.2

QUESTION 8

An AP is advertised as a tri-band, 4x4:4, Wi-Fi 6, 802. 11ax AP. Based on this information and assuming it is correctly advertised, what can be determined as certainly true about this AP?

A. It supports four channels in 2.4 GHz and 4 channels in 5 GHz

B. It supports UL-MU-MIMO

C. It uses a modified OpenWRT firmware

D. It has 4 radio chains

Correct Answer: D

Based on the information given, what can be determined as certainly true about this AP is that it has 4 radio chains. A radio chain is a hardware component that consists of an antenna, a radio frequency (RF) amplifier, and a transceiver. The

number of radio chains indicates how many spatial streams an AP can transmit or receive simultaneously using Multiple Input Multiple Output (MIMO) technology. The notation x:y:z in an AP specification denotes the number of radio chains

(x), the number of spatial streams (y), and the number of spatial streams per band (z). Therefore, a tri-band, 4x4:4, Wi-Fi 6, 802.11ax AP has four radio chains in each of its three bands (2.4 GHz, low 5 GHz, and high 5 GHz). It also supports

four spatial streams in total and four spatial streams per band. It cannot be determined as certainly true that it supports four channels in each band, UL-MU-MIMO, or uses a modified OpenWRT firmware based on the information given.

References: [CWNP Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 223; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 213.

QUESTION 9

You administer a small WLAN with nine access point. As a small business, you do not rum a RADIUS server and use WPA2-Personal for security. Recently, you changed the passphrase for WPA2-personal in all Aps and clients. Several users are now reporting the inability to connect to the network at time and it is constrained to one area of the building. When using scanner, you see that the AP covering that area is online

A. The AP that covers the problem area requires a firmware update

B. The clients are improperly configured

C. The AP that covers the problem area has failed

D. The AP that covers the problem area is improperly configured

Correct Answer: B

This is because the passphrase for WPA2-Personal is case-sensitive and must match exactly on both the AP and the client. If the passphrase is entered incorrectly on the client, the client will not be able to authenticate with the AP and connect to the network. The AP that covers the problem area is not likely to require a firmware update, fail, or be improperly configured, as it is online and works with other clients that have the correct passphrase. To troubleshoot this issue, you can check the passphrase settings on the clients and make sure they matchwith the AP. You can also try to reconnect the clients to the network or reboot them if necessary. For more information on how to configure WPA2-Personal on your router

QUESTION 10

In an 802.11 2.4 GHz system, what 22 MHz channels are considered non-overlapping?

A. 7 and 11

B. 2 and 8

C. 1 and 5

D. 4 and 6

Correct Answer: C

In the 2.4 GHz frequency band used for 802.11 wireless networks, the channel bandwidth is typically 20 MHz, but the actual frequency spread of each channel is about 22 MHz due to the modulation techniques used. This spread causes

overlap between adjacent channels, which can lead to interference and degrade network performance. To avoid this, it\\'s essential to use non-overlapping channels.

The three non-overlapping channels in the 2.4 GHz band are 1, 6, and 11. Each of these channels is spaced sufficiently apart to avoid interference with each other:

Channel 1: Centered at 2.412 GHz.

Channel 6: Centered at 2.437 GHz.

Channel 11: Centered at 2.462 GHz.

Given the options provided, option C (1 and 5) is the closest to a pair of non-overlapping channels, although in practice, channel 5 would still cause some interference with channel 1 due to the 22 MHz spread. The ideal choice for non-

overlapping channels would be any two channels among 1, 6, and 11, but this is not an option provided. Therefore, within the given options, 1 and 5 are the best choice, understanding that in a real-world scenario, 1 and 6 or 6 and 11 would

be preferred to avoid overlap.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Understanding 2.4 GHz channel arrangement and interference patterns in 802.11 wireless networks.

QUESTION 11

What is appended to the end of each 802.11 data frame after the payload?

A. Preamble

B. MAC header

C. PHY header

D. FCS

Correct Answer: D

The FCS (Frame Check Sequence) is appended to the end of each 802.11 data frame after the payload. The FCS is a 4-byte field that contains a CRC-32 (Cyclic Redundancy Check) value that is calculated based on the contents of the MAC header and the payload of the frame. The FCS is used by the receiver to verify the integrity of the frame and to detect any errors or corruption that may have occurred during transmission. If the FCS does not match with the expected value, the frame is discarded by the receiver. References: , Chapter 4, page 139; , Section 4.2

QUESTION 12

Lynne runs a small hotel, and as a value added service for his customers he has implemented a Wi-Fi hot-spot. Lynne has read news articles about how hackers wait at hot- spots trying to take advantage of unsuspecting users. He wants to avoid this problem at his hotel.

What is an efficient and practical step that Lynne can take to decrease the likelihood of active attacks on his customers\\' wireless computers?

A. Enable station-to-station traffic blocking by the access points in the hotel.

B. Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.

C. Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.

D. Require EAP-FAST authentication and provide customers with a username/password on their receipt.

Correct Answer: A

In a public Wi-Fi hotspot, like the one Lynne runs in his hotel, ensuring customer security against active attacks is crucial. Active attacks involve unauthorized access, eavesdropping, or manipulation of the network traffic. To mitigate such

threats, an effective and practical step is:

Station-to-Station Traffic Blocking: Also known as client isolation, this feature prevents direct communication between devices connected to the Wi-Fi network. By enabling this on the access points, Lynne can significantly decrease the

likelihood of active attacks like man-in-the-middle (MITM) attacks, where an attacker intercepts and possibly alters the communication between two parties. The other options, while beneficial for network security, might not be as

straightforward or practical for Lynne\\'s situation:

Network Access Control (NAC)requires a more complex infrastructure and management, which might not be ideal for a small hotel setup. Implementing an SSL VPNadds an extra layer of security but might complicate the login process for

users, potentially affecting the user experience. Requiring EAP-FAST authenticationprovides secure authentication but may not be feasible for transient customers who expect quick and easy network access. Therefore, enabling station-tostation traffic blocking is a practical and efficient measure that Lynne can implement to enhance customer security on the Wi-Fi network.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Best practices for securing a wireless network in a public hotspot environment.

QUESTION 13

You support a WLAN using dual-band 802.11ac three stream access points. All access points have both the 2.4 GHz and 5 GHz radios enabled and use 40 MHz channels in 5 GHz and 20 MHz channels in 2.4 GHz. A manager is concerned about the fact that each access point is connected using a 1 Gbps Ethernet link. He is concerned that the Ethernet link will not be able to handle the load from the wireless radios. What do you tell him?

A. His concern is valid and the company should upgrade all Ethernet links to 10 Gbps immediately.

B. His concern is valid and the company should immediately plan to run a second 1 Gbps Ethernet link to each AP.

C. His concern is invalid because the AP will compress all data before transmitting it onto the Ethernet link.

D. Due to 802.11 network operations and the dynamic rates used by devices on the network, the two radios will likely not exceed the 1 Gpbs Ethernet link.

Correct Answer: D

What you should tell him is that due to 802.11 network operations and the dynamic rates used by devices on the network, the two radios will likely not exceed the 1 Gbps Ethernet link. This is because the actual throughput of an 802.11 network is much lower than the theoretical data rates due to factors such as overhead, contention, interference, retransmissions, and environmental conditions. Moreover, the data rates used by devices on the network vary depending on their distance, signal quality, capabilities, and configuration. Therefore, it is unlikely that both radios of the AP will simultaneously use the maximum data rates and saturate the 1 Gbps Ethernet link. Upgrading to a 10 Gbps Ethernet link or running a second 1 Gbps Ethernet link may be unnecessary and costly. Compressing all data before transmitting it onto the Ethernet link may introduce additional overhead and latency. References: [CWNP CertifiedWireless Network Administrator Official Study Guide: ExamCWNA-109], page 227; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 217.

QUESTION 14

When compared with legacy Power Save mode, how does VHT TXOP power save improve battery life for devices on a WLAN?

A. Legacy Power Save mode was removed in the 802.11ac amendment.

B. VHT TXOP power save allows the WLAN transceiver to disable more components when in a low power state.

C. VHT TXOP power save uses the partial AID in the preamble to allow clients to identify frames targeted for them.

D. VHT TXOP power save allows stations to enter sleep mode and legacy Power Save does not.

Correct Answer: B

VHT TXOP (Very High Throughput Transmit Opportunity) power save is a feature introduced with the 802.11ac amendment, which is designed to improve the power efficiency of devices connected to a WLAN. This feature enhances battery

life in several ways, compared to the legacy Power Save mode:

Enhanced Power Saving: VHT TXOP power save allows devices to disable more components of the WLAN transceiver when they are in a low power state. This reduces the power consumption during periods when the device is not actively

transmitting or receiving data.

Intelligent Wake-Up Mechanisms: It employs more sophisticated mechanisms for devices to determine when they need to wake up and listen to the channel, further reducing unnecessary power usage.

Optimized Operation: This power save mode is optimized for the high-throughput environment of 802.11ac networks, allowing devices to efficiently manage power while maintaining high performance.

Legacy Power Save mode, introduced in earlier versions of the 802.11 standards, does not provide the same level of component disablement or the intelligent wake-up mechanisms found in VHT TXOP power save, making option B the

correct answer.

References:

IEEE 802.11ac-2013 Amendment: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott.

QUESTION 15

When implementing PoE, what role is played by a switch?

A. PSE

B. Midspan injector

C. PD

D. Power splitter

Correct Answer: A

PoE stands for Power over Ethernet, which is a technology that allows network devices to receive power and data over the same Ethernet cable. PoE eliminates the need for separate power adapters or outlets for devices such as IP phones, cameras, or APs. PoE requires two types of devices: PSE (Power Sourcing Equipment) and PD (Powered Device). A PSE is a device that provides power to the Ethernet cable, such as a switch, injector, or splitter. A PD is a device that receives power from the Ethernet cable, such as an IP phone, camera, or AP. When implementing PoE, a switch plays the role of a PSE910. References: CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 293; CWNA109Study Guide, Chapter 7: Power over Ethernet (PoE), page 287.